

**APPLICANTS INTERVIEW SUMMARY**

On May 31, 2007, a telephone interview was held between Examiner Carlton Johnson, Examiner Taghi Arani, and Applicants' attorney Oliver Ong (Reg. No. 58,456). The interview was held in order to address the 35 U.S.C. § 112 rejection regarding claims 20, 34, 26, and 40. Applicants' attorney pointed to sections of the Applicants' specification that supported the claim amendments submitted in the last response, and the Examiners agreed that the cited description support overcomes the § 112 rejection.

Applicants' attorney also discussed the limitations of claims 20, 24, 26, 40, 29, and 43 with respect to the cited references of Yeager et al. or Yellepeddy and the 35 U.S.C. §§ 102 and 103 rejections.

Regarding claims 20 and 24 the Examiners proposed an amendment to indicate that the administrator is different from the second member. The Examiners further proposed providing in a response language describing the delegation aspect of claim 20 and agreed that this would place claim 20 in better form for allowance.

Regarding claims 26 and 40, the Examiners proposed an amendment to further clarify the language of "providing security related information." Applicants' attorney agreed to consider a clarifying amendment.

Regarding claims 26, 40, 29 and 43, Applicants' attorney explained that Yeager et al. does not describe publishing records or a publishing a token and with respect to claims 29 and 43, that Yellpeddy et al. does not describe publishing a revocation record.

While no specific agreement was reach with respect to the claims, the Examiner agreed to review the case in light of the discussion and indicated that a further search may be performed based on the discussed subject matter. The Examiner requested that the Applicants submit a response to the office action for consideration.

**REMARKS****35 U.S.C. § 112**

Applicants respectfully traverse the rejection of claims 20 and 34 under 35 U.S.C. § 112, first paragraph, based on a disclosure that is not enabling. Each of claims 20 and 34 recites receiving a certificate renewal request at a second member in the group from a first member, and requesting by the second member authorization from an administrator different from the second member for renewing the certificate. This limitation is supported at least by Figure 1 and corresponding paragraph 0104:

Referring now to FIG. 7, a flow diagram illustrates a method for performing online renewal. Block 710 provides that GSM 210 receives a request from a group member seeking renewal of a GMC.... Block 720 provides that GSM 210 uses membership record and the graphing presence record to find an active administrator. Block 730 provides that GSM 210 searches for administrators using the membership record. For a given administrator, block 740 provides that GSM 210 then determines using the presence record if that administrator is online or not. If that administrator is online, block 750 provides that GSM 210 establishes a point to point connection to that administrator so that the group member who has to renew the certificate can send its GMC.... Paragraph 0104 of Applicants Specification

It is important to note that in a peer to peer network, an application such as a group security manager (GSM) is considered a graph client. (See paragraphs 0031 and 0034). Thus, the claimed limitation is fully supported by the specification and the § 112 rejection should be withdrawn.

Applicants respectfully traverse the rejection of claims 26 and 40 under 35 U.S.C. § 112, first paragraph, as based on a non-enabling disclosure. Each of claims 26 and 40 recites a token that is published in a graph database, where the graph database makes available security related information including the published token to each member of the secure group. Because a graph is a group of peer nodes (see paragraph 0030), a graph database is the same as a group database. A group database is disclosed in paragraph 0091 to store security related information. Paragraph 0091 further discloses that the group database operates to allow every group member to receive the security information when published. A token is disclosed in paragraph 0049 to contain information about the roles of a publisher and

security related information is described to contain the role information at paragraphs 0048-0049. Moreover, paragraph 0122 describes that a group membership certificate (GMC) is a token which is necessary to validate a record published by a member. Thus, the limitation of a token that is published in a graph database where the graph database provides security related information including the published token to each member of the secure group is fully supported by the specification and the § 112 rejection should be withdrawn.

### 35 U.S.C. § 102

#### Claims 26, 28, 40 and 42

Applicants respectfully traverse the rejection of claims 26, 28, 40 and 42 as anticipated by Yeager et al. (U.S. Publication No. 2005/0086300). Each of claims 26, 28-31, 40 and 42-45 recites publishing a token of a publisher (e.g., a member publishing a record) in a graph database that makes available the published token to each member of a graph database and matching the published token against a security descriptor for a record to be published. Yeager et al. does not disclose a graph database that makes available a publisher's token to each member of a secure group or matching a security descriptor of a record to be published against the published token.

While Yeager et al. discloses sending a token with a message to a recipient at paragraph 0577, Yeager et al. does not disclose checking a security descriptor for a record against a publishers token made available by a graph database to each member of a group. In particular, Yeager et al. at paragraph 0577 discloses that a token is included in a message body and can be used to verify the sender's right to send the message to a particular member.

.... A credential is a token that when presented in a message body is used to identify a sender and can be used to verify that sender's right to send the message to the specified endpoint ....  
The sending address placed in the message envelope may be crosschecked with the sender's identity in the credential....  
Paragraph 0577 of Yeager et al.

At best, this passage describes that a security descriptor is included in a message body. However, this paragraph does not disclose checking a security descriptor against a publishers token made available by a graph database to each member of a group. In fact, paragraph 0577 discloses that the token/credential information contained in a message body is used to check the sending address in the message envelope. Thus, the message appears to

be a self-certifying message that does not require secondary credentials (such as a token made available by a graph database) for validation.

Because Yeager et al. does not disclose a graph database that makes available security information including a publishers token to each member of a secure group or checking a security descriptor of a record to be published against the publishers token in the graph database, Yeager et al. does not anticipate claims 26, 28, 40 and 42.

*Claims 29-31 and 43-45*

Applicants respectfully traverse the rejection of claims 29-31 and 43-45 as anticipated by Yeager et al. Each of claims 29-31 and 43-45 recites publishing a revocation record to a group where the revocation record identifies a member of a group and revoking any records published by the member according to the revocation record.

Yeager et al. does not disclose a record that identifies a member of a group whose published records are or will be revoked. In particular, the Office action cites paragraph 0086 that discloses a memory for storing a program that implements a peer, paragraph 0223 for a system that is capable of publishing content, and paragraph 0558 for a system that is able to revoke membership. However, none of the paragraphs cited by the Office action remotely disclose publishing a record that identifies a member of a group whose published records are revoked or will be revoked. Therefore, Yeager et al. does not anticipate claims 29-31 and 43-45.

**35 U.S.C. § 103**

*Claims 20, 21, 34 and 35(Yeager et al. in view of Yellepeddy)*

Applicants respectfully traverse the rejection of claims 20, 21, 34, and 35 as obvious over Yeager et al. in view of Yellepeddy et al. (U.S. Patent No. 2004/0111607). Each of claims 20 and 34 recites receiving a certificate renewal request at a second member in the group from the first member and requesting by the second member authorization from an administrator different from the second member for renewing the certificate. Thus, each of the claims recite a certificate renewal request of a first entity (i.e., the first member) being received at a second entity (i.e., the second member) and the second entity requesting authorization from a third entity (i.e., the administrator) for renewing the certificate.

The office action acknowledges that Yeager et al. does not disclose a certificate renewal process, nor is Yeager et al. cited for this purpose. Instead, the office action relies on Yellepeddy et al. to disclose the claimed renewal process. However, Yellepeddy et al. does not disclose a certificate renewal request from a first member being received at a second member and the second requesting authorization from an administrator different from the second member for renewing the certificate.

Generally, the claimed renewal process of claims 20, 21, 34 and 35 is implemented in a peer to peer network in which one peer acts on behalf of another peer to initiate a renewal process. The cited paragraph 0092 of Yellepeddy et al. merely discloses a process in which multiple certificate authorities (called OSCP responders) have their shared public certificate updated so that none of certificate authorities have an expired public certificate (which would make a certificate authority inoperative). In fact, none of certificate authorities of Yellepeddy et al. request a certificate renewal, but instead, a master authority (called a master OSCP responder) automatically renews the group certificate of each certificate authority without being prompted by any of the certificate authorities. Thus, Yellepeddy et al. does not disclose or teach a second member that receives a certificate renewal request from a first member, much less a second member that receives a certificate renewal request from a first member and that requests authorization from a third member (an administrator) for renewing the certificate. Because neither Yeager et al. nor Yellepeddy et al. disclose the claimed renewal process, no combination of Yeager et al. and Yellepeddy et al. can render claims 20, 21, 34, and 35 obvious.

*Claims 22-25 and 36-39 (Yeager et al. in view of Yellepeddy)*

Applicants respectfully traverse the rejection of claims 22-25 and 36-39 as obvious over Yeager et al. in view of Yellepeddy. Each of claims 22-25 and 36-39 recites receiving a request to renew a certificate that is published in a graph database, and performing renewal of the published certificate. Neither Yeager et al. nor Yellepeddy et al. disclose receiving a request to renew a certificate that is published in a graph database, and thus, no combination of Yeager et al. and Yellepeddy et al. can render claims 22-25 and 36-39 obvious.

The Office action acknowledges that Yeager et al. does not disclose renewing a certificate. Instead, the Office action relies on Yellepeddy to disclose to remedy the

deficiency. However, Yellepeddy also does not disclose receiving a request to renew a certificate that is published in a graph database.

While Yellepeddy discloses a certificate renewal process, the Yellepeddy renewal process does not publish a certificate marked for renewal in a graph database. In fact, Yellepeddy et al. fails to disclose a graph database, in any manner. Instead, Yellepeddy discloses a system in which a master certificate authority (called a master OCSP responder) renews a group certificate of a set of subordinate certificate authorities without receiving a request for renewal. See paragraph 0086. Thus, Yellepeddy does not disclose a request for renewing a certificate, much less a request for renewing a certificate that is published in a graph database. Because neither Yeager et al. nor Yellepeddy discloses receiving a request to renew a certificate that is marked for renewal and published in a graph database, no combination of Yeager et al. and Yellepeddy can render claims 22-25 and 36-39 obvious.

*Claims 32, 33, 46, and 47 (Yeager et al. in view of Aguilera et al.)*

Applicants respectfully traverse the rejection of claims 32, 33, 46, and 47 as obvious over Yeager et al. in view of Aguilera et al. (U.S. Publication No. 2004/0243827). Each of claims 32, 33, 46, and 47 recites a revocation bit map comprising one or more bits that identify one or more members of a group and altering one or more bits of the revocation bit map to revoke one or more members of the group. Neither Yeager et al. nor Aguilera et al. disclose or teach a revocation bit map having bits that identify members of a group or altering the bits of the bit map to revoke one or more members of a group. Therefore, no combination of Yeager et al. and Aguilera et al. can render claims 32, 33, 46, and 47 obvious.

The Office action acknowledges that Yeager et al. fails to disclose using a bit map to revoke a member of a group, nor is Yeager et al. cited for this purpose. Instead, the office action relies on Aguilera et al. to disclose the recited limitation. However, Aguilera et al. also does not disclose a revocation bit map having one or more bits that identify one or more members of a group. Instead, Aguilera et al. discloses a capabilities list and a revocation list that do not identify individual members of a group for revocation.

Generally, Aguilera et al. discloses using a capabilities revocation list and a group list containing a list of valid groups (listed by name of the group, not by individual members of the group) corresponding to granted capabilities to determine whether a client has the right or privilege to execute a function (such as a request to access data). See paragraph 0004 and

0013. Aguilera et al. further discloses that if a client is requesting execution of a function that is on the capabilities revocation list, then the client will be unable to execute the function. Aguilera et al. also discloses that a capability may be revoked for a group having the capability by invalidating the group in the group list. Neither one of these lists, however, list elements or bits that correspond to individual members of a group. Because neither of the Aguilera lists contain elements that correspond to members of a group, no alteration of the bits of a bitmap derived from the Aguilera lists can result in revoking members of a group. Because neither Yeager et al. nor Aguilera et al. disclose a bit map having bits that identify a member, no combination of Yeager et al. and Aguilera et al. can render claims 32, 33, 46, and 47 obvious.

### CONCLUSION

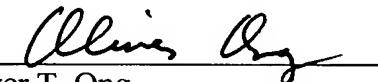
For the foregoing reasons, Applicants respectfully request reconsideration and withdrawal of the rejections/objections and allowance of claims 20-26, 28-40, and 42-47.

The Commissioner is authorized to charge any fee deficiency required by this paper, or credit any overpayment, to Deposit Account No. 13-2855.

If there are matters that can be discussed by telephone to further the prosecution of this application, Applicants respectfully request that the Examiner call its attorney at the number listed below.

Dated: July 5, 2007

Respectfully submitted,

By   
Oliver T. Ong

Registration No.: 58,456  
MARSHALL, GERSTEIN & BORUN LLP  
233 S. Wacker Drive, Suite 6300  
Sears Tower  
Chicago, Illinois 60606-6357  
(312) 474-6300  
Attorney for Applicant